PATENT

SYSTEM AND METHOD FOR SECURE DATA TRANSFER OVER A NETWORK

RELATED APPLICATIONS

[0001]   This application is related to and shares a common disclosure with commonly-assigned copending applications U.S. Application No. 10/_____, titled "System and Method for Performing Security Operations on Network Data" and U.S. Application No. 10/_____, titled "System and Method for Performing Cryptographic Operations on Network Data", both filed on February __, 2004, the entire contents of which are incorporated here by reference.

BACKGROUND

[0002]   Today, most data transfers sent over the public networks, such as the Internet, are left unprotected against attacks. Even users of private networks that rely on public network communication facilities to connect end-user terminals and workstations in the private network to servers and other terminals in the public network are vulnerable to attacks. Moreover, recent industry studies have found that over half of all private network security breaches originated from within the private network. The situation results mainly because popular packet communication protocols, such as TCP/IP, do not have protection mechanisms designed into their protocol stacks. Consequently, any terminal connected to a TCP/IP network can intercept, replay, or produce IP packets sent over the network.

[0003]   In response to the situation, the Internet Engineering Task Force (or IETF) defined Internet Protocol Security (or IPSec) to provide encryption-based security in TCP/IP networks. IPSec is a network-layer (e.g., the IP layer of TCP/IP) security

Att'y Docket No. RPS9-2002-0014   1